IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re patent application of:	) Attorney Docket No.: F-240
	) Customer No.: 00919
Douglas B. Quine	)
	) Examiner: Tommy D. Lee
Serial No.: 09/748,994	) Group Art Unit: 2625
Filed: December 27, 2000	)
Confirmation # 6431	) Date: February 6, 2008

Title: A METHOD FOR VERIFYING THE AUTHENTICY OF AN ELECTRONIC DOCUMENT

Mail Stop Appeal Brief- Patents
Commissioner for Patents
Alexandria, VA 22313-1450

APPELLANT'S BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 41.31 et seq. from the final rejection of claims 1, 5, 7, 12-23 and 25 of the above-identified application mailed September 6, 2007. This Brief is in furtherance of the Notice of Appeal transmitted in this case on December 6, 2007. A petition and fee for a two-month extension of time is submitted herewith. Accordingly, this brief is timely filed. The fee for submitting this Brief is $510.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of $510.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required for this appeal or to make this brief timely or credit any overpayment to Deposit Account No. **16-1885**.

TABLE OF CONTENTS

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

There are no appeals or interferences known to Appellants, their legal representative, or the assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. Status of Claims

Claims 1, 5, 7, 12-23 and 25 are in the case and under final rejection of the Examiner.

Claims 2-4, 6, 8-11 and 24 are canceled.

Claims 1, 5, 7, 12-23 and 25 are in the case and stand finally rejected under 35 U.S.C. 103(a) as allegedly rendered obvious by U.S. Patent No. 5,438,433 to Reifman, et al. ("Reifman '433") in view of U.S. Patent No. 6,170,744 to Lee, et al. ("Lee '744").

Appellants hereby appeal the final rejection of claims 1, 5, 7, 12-23 and 25.

IV. Status of Amendments

There are no amendments to the claims filed subsequently to the Final Office Action of September 6, 2007. Therefore, the claims set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Claimed Subject Matter

Appellants' invention as presently claimed relates generally to a new and useful method for verifying the authenticity of received documents by computing an encrypted checksum of the document transmitted and comparing a decrypted checksum of the document received at the destination device with the encrypted checksum value calculated at the originating device. See Specification at p. 1, lines 110-17.

Certain illustrative embodiments describe a new and useful system for authenticating a facsimile document communicated between a first facsimile communication device via a communications network including marking a print out to indicate a taper condition. An originating facsimile apparatus 210 scans an original input document 205 and coverts it into a digitalized file format. Furthermore, the facsimile apparatus 210 is provided with a capability to calculate a checksum of the original input document 205, and encrypt the same prior to transmission to one of a plurality of destination devices 220, 230. See FIG. 2A and specification at p. 6, ll. 3-14.

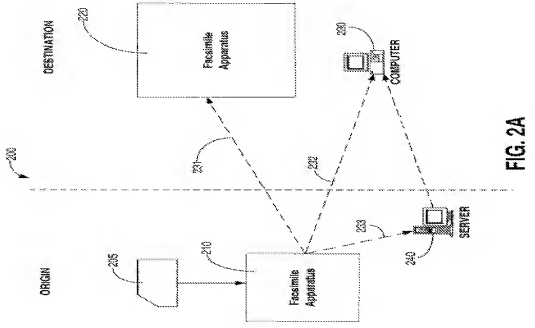

FIG. 2A

Checksum of a document 205 may be determined using any of the known checksum algorithms including Secure Hash Algorithms (SHA). The facsimile apparatus 210 includes a system for convolving the original input data converted into a digital file format and the encrypted checksum data in order to produce a convolved data for transmission to one or more of destination devices 220, 230. The convolved data may be transmitted via communication links 231, 232, or 233 to destination devices 220, 230, 240 respectively. The receiving/destination facsimile apparatus 220

is capable of receiving the convolved data transmitted by the facsimile apparatus 210. Facsimile apparatus 220 is capable of performing all the operations performed by facsimile apparatus 210, but in reverse order in order to retrieve the data transmitted by facsimile apparatus 210. Thus, facsimile apparatus 220 includes the capability to decrypt the encrypted checksum data and compare the decrypted checksum data against the checksum data calculated by facsimile apparatus 220 on the destination side. In the event of a mismatch, the facsimile apparatus 220 includes capability to alert a recipient of the transmission, at the destination side, about the mismatch of the checksum data. One form of indicating a recipient would be by placing a large "X" mark on a portion of the document received by the facsimile apparatus 220, the document representing original document data transmitted from facsimile apparatus 210 at the origin. See FIG. 2A and specification at p. 6, l. 15- p. 8, l. 12.

FIG. 2B shows a clearly marked output documents indicating a tamper condition on facsimile 270. See FIG. 2B and specification at p. 10, ll. 8-19.

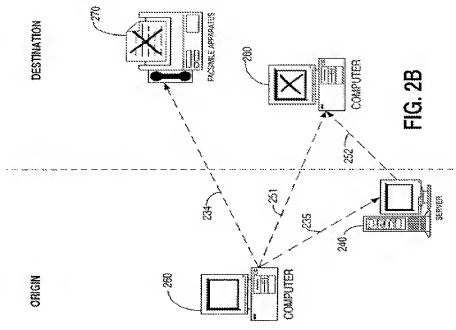

FIG. 2B

FIG. 3A, shows a process overview for the security verification performed by an intelligent digital facsimile apparatus 361 that is functionally similar to the facsimile apparatus 220 as represented in FIG. 2A, and facsimile apparatus 270 as represented in FIG. 2B. An integrity check of a document received by a recipient at a destination device, such as facsimile apparatus 361, is made by decrypting the encrypted checksum and comparing this decrypted checksum with a checksum of the document received by facsimile apparatus 361. In the event of a mismatch, a portion of the document received by facsimile apparatus is clearly marked to denote that the received document has been tampered with. See FIG. 3A and specification at p. 10, l. 19- p. 11, l. 8.

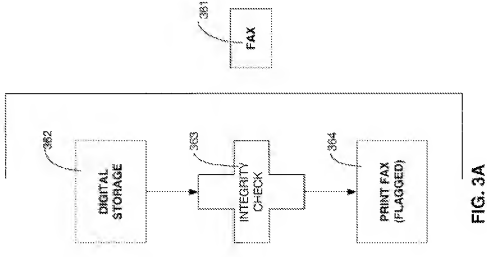

FIG. 3A

Independent claim 1 is shown with illustrative annotated reference to the specification, reference numerals and figures that are not intended to be exhaustive:

1. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of (FIG.2A, 3A, page 3, ll. 14-17):

a. receiving input data representing the entire facsimile document and generating facsimile information in a first format by said first communication device from said input data (FIG.2A, 3A, 210, 205, page 6, ll. 9-14);

b. processing said input data, at said first communication device, to compute an encrypted checksum of the entire input data (FIG.2A, 3A, 210, 205, page 6, l. 11- page 7, l. 8);

c. convolving said facsimile information with said encrypted checksum data to produce convolved data (FIG.2A, 3A, 210, 205, page 7, ll. 9-29);

d. decrypting, at said second communication device, said encrypted checksum (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);

e. computing a checksum of said input data received at said second communications device (FIG.2A, 3A, 220, 361, page 8, ll. 2-7); and

f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d) by clearly marking a print out of the received input data indicating a tamper condition (FIG.2A, 3A, 220, 361, 270, page 8, ll. 7-12).

Independent claim 15 is shown with illustrative annotated reference to the specification, reference numerals and figures that are not intended to be exhaustive:

15. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of (FIG.2A, 3A, page 3, ll. 14-17):

receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the digital representation of the entire facsimile document in a first format sent by said first communication device (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);

processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);

decrypting, at said second communication device, said encrypted authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);

computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-7); and

alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data by clearly marking a print out of the received input data indicating a tamper condition. (FIG.2A, 3A, 220, 361, 270, page 8, ll. 7-12).

Independent claim 23 is shown with illustrative annotated reference to the specification, reference numerals and figures that are not intended to be exhaustive:

> 23. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of (FIG.2A, 3A, page 3, ll. 14-17):
>
> receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the facsimile document and consisting of a single encrypted checksum of the entire facsimile document in a first format sent by said first communication device (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);
>
> processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data;
>
> decrypting, at said second communication device, said encrypted authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-7);
>
> computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-7); and
>
> alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data (FIG.2A, 3A, 220, 361, page 8, ll. 2-12),
>
> wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a mark across a print out of the received input data clearly indicating a tamper condition (FIG.2A, 3A, 220, 361, 270, page 8, ll. 7-12).

Additional features of the invention are discussed below in the Argument section of this Brief. This summary is not intended to supplant the description of the claimed subject matter as provided in the claims as recited in Appendix A, as understood in light of the entire specification.

VI. Grounds of Rejection to Be Reviewed on Appeal

Whether claims 1, 5, 7, 12-23 and 25 are patentable under 35 U.S.C. §103(a).

VII. Argument

As discussed in detail below, Appellant respectfully submits that the final rejection of claims 1, 5, 7, 12-23 and 25 does not meet the threshold burden of presenting a prima facie case of unpatentability. Accordingly, Appellant is entitled to grant of those claims. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

A Claims 1, 5, 7, 12-23 and 25 are not Unpatentable under 35 U.S.C. § 103(a)

Claims 1, 5, 7, 12-23 and 25 are in the case and stand rejected under 35 U.S.C. 103(a) as allegedly rendered obvious by U.S. Patent No. 5,438,433 to Reifman, et al. ("Reifman '433") in view of U.S. Patent No. 6,170,744 to Lee, et al. ("Lee '744").

Appellant respectfully disagrees with the rejection and urge its reversal for at least the reasons stated below.

In rejecting a claim under 35 U.S.C. §103, the Examiner is charged with the initial burden for providing a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 375 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference and/or combine applied references to arrive at the claimed invention. *In re Ochiai*, 37 USPQ2d 1127 (Fed. Cir. 1995); *In re Deuel*, 51 F.3d 1552, 34 USPQ 1210 (Fed. Cir. 1995); *In re Fritch*, 972 F.2d 1260, 23 USPQ 1780 (Fed. Cir. 1992); *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. ___ , 127 S.Ct. 1727, 1735 (2007).

Initially, Appellant respectfully submits that the references are not properly combined. Lee '744 requires the use of physical documents that are physically generated at the source and would not be operable in combination with a facsimile

system. The two references are not analogous since Reifman '433 deals exclusively with electronic facsimile document transmission and Lee '744 deals exclusively with physical document transport. Accordingly, one of skill in the art would not look to Lee '744 in order to modify Reifman '433.

Furthermore, any marking system of Lee '744 that were to be combined with Reifman '433 would not be capable of printing the entire document at the destination and thus the combination would not be operable or at least not suitable for its intended purpose. Moreover, it appears that the system of Lee '744 does not create a digital signature of an entire document.

Clearly marking the suspect output print out as currently claimed in the present invention is an important advance of the cited references since a non-expert user easily understands the mark to indicate tamper and since the printed paper output facsimile documents so marked may be understood on a standalone basis with reference to only the print out to indicate a possible tamper condition. Furthermore, in the system of the present invention as currently claimed, further generation copies of the output facsimile will carry forward the physical warning.

Furthermore, with regard to Independent claims 1, 15 and 23, Appellant respectfully submits that the cited references, even if held to be properly combined, do not render the claimed invention obvious. For example, Independent claim 1 currently recites:

> 1. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:
>
> a. receiving input data representing the entire facsimile document and generating facsimile information in a first format by said first communication device from said input data;
>
> b. processing said input data, at said first communication device, to compute an encrypted checksum of the entire input data;
>
> c. convolving said facsimile information with said encrypted checksum data to produce convolved data;
>
> d. decrypting, at said second communication device, said encrypted checksum;

e. computing a checksum of said input data received at said second communications device; and

f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d) by clearly marking a print out of the received input data indicating a tamper condition.

The cited references do not appear to describe convolving the data as claimed and marking a print out of received input data.

Appellant respectfully submits that the dependent claims are patentable over the cited references for at least the reasons described above with reference to the associated independent claim and any intervening claims.

Accordingly, Appellants respectfully submit that the Examiner has not established a prima facie obviousness rejection and that the rejection is clearly in error and should be reversed.

IX. Conclusion

In Conclusion, Appellants respectfully submit that the final rejection of claims 1, 5, 7, 12-23 and 25 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,

/George M. Macdonald/

George M. Macdonald
Reg. No. 39,284
Attorney for Appellant
Telephone (203) 924-3180

PITNEY BOWES INC.
Intellectual Property and Technology Law Department
35 Waterview Drive, P.O. Box 3000
Shelton, CT 06484-8000

VIII – CLAIMS APPENDIX
APPENDIX A

1. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

a. receiving input data representing the entire facsimile document and generating facsimile information in a first format by said first communication device from said input data;

b. processing said input data, at said first communication device, to compute an encrypted checksum of the entire input data;

c. convolving said facsimile information with said encrypted checksum data to produce convolved data;

d. decrypting, at said second communication device, said encrypted checksum;

e. computing a checksum of said input data received at said second communications device; and

f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d) by clearly marking a print out of the received input data indicating a tamper condition.

5. The method of claim 1, wherein a database system is communicatively coupled to said second facsimile communication device.

7. The method of claim 1, further comprising the step of configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.

12. The method of claim 1, wherein the convolved data is transmitted to the second facsimile communication device as an e-mail attachment.

13. The method of claim 1, further comprising:

sending the convolved data to a third facsimile communication device.

14. The method of claim 1, further comprising:

receiving a user name and password from a user with the second facsimile communication device.

15. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the digital representation of the entire facsimile document in a first format sent by said first communication device;

processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data;

decrypting, at said second communication device, said encrypted authentication data;

computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data; and

alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data by clearly marking a print out of the received input data indicating a tamper condition.

16. The method of claim 15, wherein a database system is communicatively coupled to said second facsimile communication device.

17. The method of claim 15, further comprising the step of configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.

18. The method of claim 15, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a clear mark across a print out of the received input data indicating a tamper condition.

19. The method of claim 15, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition.

20. The method of claim 15, wherein the convolved data is transmitted to the second facsimile communication device as an e-mail attachment.

21. The method of claim 15, further comprising:
sending the convolved data to a third facsimile communication device.

22. The method of claim 15, further comprising:
receiving an authorized user name and password from a user with the second facsimile communication device before providing access to the facsimile document.

23. A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the facsimile document and consisting of a single encrypted checksum of the entire facsimile document in a first format sent by said first communication device;

processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data;

decrypting, at said second communication device, said encrypted authentication data;

computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data; and

alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data,

wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a mark across a print out of the received input data clearly indicating a tamper condition.

25. The method of claim 23, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition.

Appendix IX – Evidence Appendix

None

Appendix X – Related Proceedings Appendix

None